NOTA PÚBLICA sobre o uso de criptografia em sistemas e dispositivos conectados à Internet

VERSIÓN EN ESPAÑOL | ENGLISH VERSION

O COMITÊ GESTOR DA INTERNET NO BRASIL – CGI.br, no uso das atribuições que lhe confere o Decreto nº 4.829/2003, tendo em vista a frequente divulgação de iniciativas recentes que buscam criar acesso privilegiado a conteúdo de comunicações privadas em sistemas digitais, seja através de mecanismos, processos ou ferramentas que implementem vulnerabilidades ou mesmo que corrompam sistemas criptográficos; seja através do desincentivo ou dificultação do uso de criptografia, e

CONSIDERANDO

- Que o uso de criptografia forte é muito importante para que fluxos de informação se estabeleçam de forma segura e confiável na Internet, não somente para usuários individuais, como também para empresas e órgãos públicos;

- Que a proteção de tais fluxos se encontra regulada em legislação ordinária (Lei 10.406 de 10 de janeiro de 2002 - Código Civil Brasileiro; Lei 12.965 de 23 de abril de 2014 - Marco Civil da Internet, seu Decreto regulamentador nr. 8.771/2016, art. 13, inc. IV; e Lei 13.709 de 14 de agosto de 2018 - LGPD, Lei Geral de Proteção de Dados Pessoais, entre outras), e consta também dos “Princípios para a Governança e Uso da Internet” definidos pelo CGI.br, em especial o princípio da liberdade, privacidade e direitos humanos, conforme expresso na Resolução **CGI.br/RES/2009/003/P**;

VEM A PÚBLICO

- Reafirmar a importância de se garantir a possibilidade de implementação livre e adequada de criptografia forte fim a fim, tanto para a proteção do sigilo de dados e comunicações, como para o exercício de direitos previstos na Constituição Federal e leis infraconstitucionais;

- Reafirmar que uma eventual implementação de mecanismos de acesso privilegiado por meio de ferramentas tais como “backdoors” ou “chaves-mestras”, além de poder ser inócua ante intransponibilidades de ordem técnica para a obtenção da mensagem original, pode também representar riscos maiores, ao criar brechas de segurança que poderão ser exploradas para fins maliciosos;

- Reafirmar que mecanismos criptográficos sólidos são fundamentais à integridade e segurança de sistemas digitais, ao sigilo empresarial, bem como à garantia da inimputabilidade da rede e da funcionalidade, segurança e estabilidade da Internet;

- Ressaltar que uma hipotética opção por mecanismos de criptografia vulneráveis contrariaria as melhores práticas internacionais e afetaria severamente a segurança dos usuários e dos empreendimentos na Internet, bem como poderia inibir a inovação e o surgimento de modelos de negócio.